PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-244832
(43)Date of publication of application : 02.09.1994

(51)Int.Cl. H04L 9/06
H04L 9/14
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 05-031514
(22)Date of filing : 22.02.1993

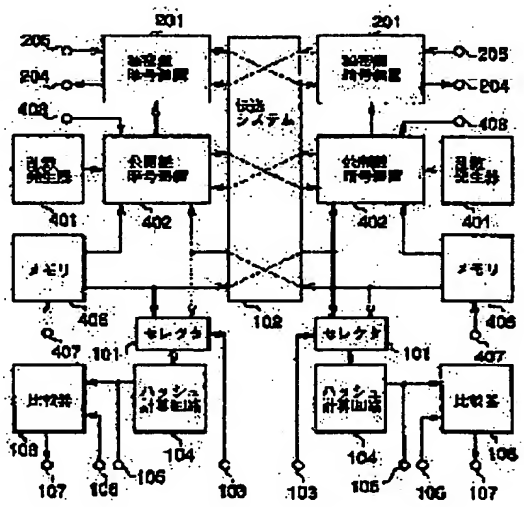
(71)Applicant : NEC CORP
(72)Inventor : SHIMADA MICHIO

(54) SECRET INFORMATION COMMUNICATION METHOD AND SECRET INFORMATION COMMUNICATION DEVICE

(57)Abstract:

PURPOSE: To prevent the communication contents from being decoded by a third party only if numerial values which are unnecessary to be kept secret and are short in figures are set to a communication device.

CONSTITUTION: A cryptographic key to be used in a secret key cryptography device 201 is ciphered in an open key cryptography device 402 and is made to be transmitted to a communication device, and further, an open key to be used in the open key cryptography device 402 is made to be transmitted and received to/from the communication device. The hash value of the open key received by the communication device is calculated in a hash calculation circuit 104, the hash value and the hash value to be supplied from an input terminal 106 are compared in a comparator 108 and a communication is terminated if the both of them do not coicide. The hash value of the open key recorded in the communication device of a communication opposite party is preliminarily supplied to the input terminal 106.



LEGAL STATUS

[Date of request for examination]	22.02.1993
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2126012
[Date of registration]	28.01.1997
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	21.02.2000

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－244832

(43)公開日　平成６年(1994)９月２日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ　9/06					
9/14					
9/00					
		7117－5K	Ｈ０４Ｌ　9/ 02	Ｚ	
		7117－5K	9/ 00	Ｚ	

審査請求　有　請求項の数５　ＯＬ　（全　９　頁）　最終頁に続く

(21)出願番号　特願平5－31514

(22)出願日　平成５年(1993)２月22日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝五丁目７番１号　日本電気株式会社内

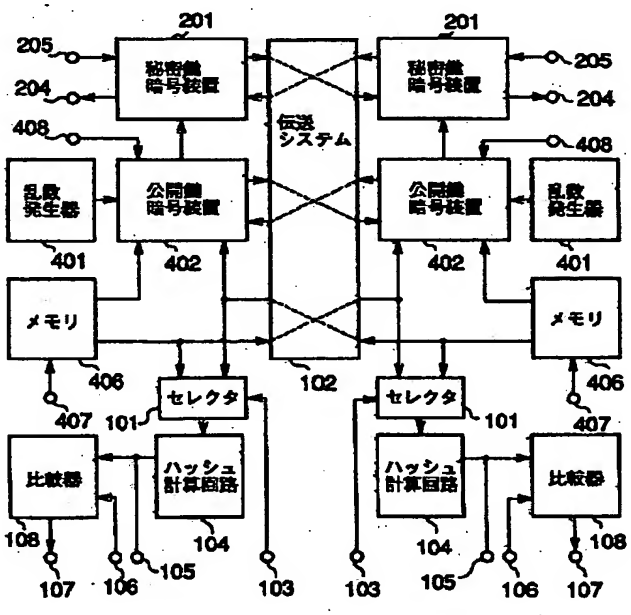
(74)代理人　弁理士　後藤　洋介　（外２名）

(54)【発明の名称】　秘密情報通信方法及び秘密情報通信装置

(57)【要約】

【目的】　秘密にする必要が無くしかも桁数の短い数値を通信装置に設定するだけで、通信内容が第三者に解読できないようにする。

【構成】　秘密鍵暗号装置２０１で使用する暗号鍵を公開鍵暗号装置４０２で暗号化して通信装置に送信させ、さらに公開鍵暗号装置４０２で使用する公開鍵を通信装置に送受信させる。そして、通信装置が受信した公開鍵のハッシュ値をハッシュ計算回路１０４で算出して、そのハッシュ値と入力端子１０６から供給されるハッシュ値とを比較器１０８で比較し、両者が一致しなければ通信を終了する。なお、入力端子１０６には、予め、通信相手の通信装置に記録されている公開鍵のハッシュ値を供給しておく。



1

【特許請求の範囲】

【請求項１】　データを秘密鍵暗号で暗号化して伝送し、秘密鍵暗号の暗号鍵を公開鍵暗号で暗号化して伝送する秘密情報通信方法において、少なくとも、公開鍵暗号の公開鍵を受信する受信ステップと、受信した公開鍵のハッシュ値を計算する計算ステップと、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを比較する比較ステップと、この比較ステップにおいて両ハッシュ値が一致しない時、通信を終了する通信終了ステップとを含むことを特徴とする秘密情報通信方法。

【請求項２】　前記通信終了ステップは、両ハッシュ値が一致しない時、通信終了指示を表示する表示ステップと、通信終了指示に応答して、通信を終了するステップとを、有することを特徴とする請求項１に記載の秘密情報通信方法。

【請求項３】　前記表示ステップは、両ハッシュ値が一致しない時、前記通信終了指示を可聴表示又は可視表示することを特徴とする請求項２に記載の秘密情報通信方法。

【請求項４】　前記比較ステップは、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを表示装置に表示させえて比較することを特徴とする請求項１に記載の秘密情報通信方法。

【請求項５】　データを秘密鍵暗号で暗号化して伝送し、秘密鍵暗号の暗号鍵を公開鍵暗号で暗号化して伝送する秘密情報通信装置において、少なくとも、公開鍵暗号の公開鍵を受信する受信手段と、受信した公開鍵のハッシュ値を計算する計算手段と、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを比較する比較手段と、この比較手段において両ハッシュ値が一致しない時、通信を終了する通信終了手段とを含むことを特徴とする秘密情報通信装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、電話やファクシミリやモデムなどの通信装置において、送信するデータを暗号化して第三者によってデータが解読されないようにするための秘密情報通信方法に関する。本発明は、更に、この秘密情報通信方法を実行する秘密情報通信装置に関する。

【０００２】

【従来の技術】通信内容が盗聴されても伝送データから送信したデータが解読されないように、データを暗号化して伝送する秘密情報通信装置としては、秘密鍵暗号にもとづく装置と公開鍵暗号にもとづく装置が広く知られ使われていた。秘密鍵暗号は対称暗号とも呼ばれ、データを暗号化するのに用いる暗号鍵と暗号化されたデータから元のデータを復号化するのに用いる暗号鍵が等しいものである。一方、公開鍵暗号は非対称暗号とも呼ばれ、データを暗号化するのに用いる暗号鍵と暗号化されたデータから元のデータを復号化するのに用いる暗号鍵とが異なるものである。公開鍵暗号では、復号化用の暗号鍵を決めると、それに対応する暗号化用の暗号鍵が簡単に算出できるが、暗号化用の暗号鍵からは復号化用の暗号鍵を算出できない。このため、暗号化用の暗号鍵を秘密にしなくとも、伝送データから送信内容が解読されない。この性質故に、暗号化用の暗号鍵および復号化用の暗号鍵は、それぞれ公開鍵および秘密鍵とも呼ばれる。なお、秘密鍵暗号や公開鍵暗号の一般的な原理や性質については、例えば、日経マグロウヒル社から昭和６０年１２月５日に出版されたデビアスとプライス（D. W. Ｄａｖｉｅｓ　ａｎｄW. L. Ｐｒｉｃｅ）著「ネットワーク・セキュリティ」などに詳しい解説がある。

【０００３】図２は、秘密鍵暗号にもとづく秘密情報通信装置の基本構成を示すブロック図である。図において秘密鍵暗号装置２０１は、入力端子２０３から供給される暗号鍵で、入力端子２０５から入力されるデータに対して秘密鍵暗号の暗号化を行い、暗号化されたデータを伝送システム２０２に出力する。一方、秘密鍵暗号装置２０１は、入力端子２０３から供給される暗号鍵で、伝送システム２０２から入力されるデータに対して秘密鍵暗号の復号化を行い、復号化されたデータを出力端子２０４から出力する。伝送システム２０２は、秘密鍵暗号装置２０１から出力されるデータをもう一方の秘密鍵暗号装置２０１に供給する。なお、例えば公衆回線用のファクシミリにおいて図２の秘密情報通信装置を用いる場合には、伝送システム２０２は変復調装置と公衆回線網によって構成されるが、本発明においては、伝送システム２０２がどのように構成されていても構わない。また、入力端子２０３に供給される暗号鍵は、図２の秘密情報通信装置の搭載された通信装置の使用者が、予め通信相手と打ち合わせて、通信相手が使う暗号鍵と等しいものを供給するものとする。

【０００４】図３は、図２の秘密情報通信装置において使われる、秘密鍵暗号装置２０１の基本構成を示すブロック図である。図において暗号化回路３０１は、入力端子２０３から供給される暗号鍵で、入力端子２０５から入力されるデータに対して秘密鍵暗号の暗号化を行い、暗号化されたデータを出力端子３０３から出力する。出力端子３０３から出力されたデータは図２の伝送システム２０２に供給されている。復号化回路３０２は、入力端子２０３から供給される暗号鍵で、入力端子３０４から入力されるデータに対して秘密鍵暗号の復号化を行い、復号化されたデータを出力端子２０４から出力する。入力端子３０４には図２の伝送システム２０２からデータが供給されている。

【０００５】なお、図３の暗号化装置で使われる秘密鍵

暗号としては、例えば、前記デビアスとプライスの書籍に解説されているＤＥＳ（Ｄａｔａ　ＥｎｃｒｙｐｔｉｏｎＳｔａｎｄａｒｄ：データ暗号化規格）暗号や、１９９２年１１月に水上で開催された情報理論とその応用シンポジウムの予稿集の２５９頁～２６０頁に記載された島田道雄著「多重剰余暗号」で述べられている多重剰余暗号がある。多重剰余暗号の暗号化および復号化を実行するための回路の構成方法は、特願平４－１２８４０９号明細書の暗号通信装置に記載されている。

【０００６】図４は、公開鍵暗号にもとづく秘密情報通信装置の基本構成を示すブロック図である。図において秘密鍵暗号装置２０１は、公開鍵暗号装置４０２から供給される暗号鍵で、入力端子２０５から入力されるデータに対して秘密鍵暗号の暗号化を行い、暗号化されたデータを伝送システム４０３に出力する。一方、秘密鍵暗号装置２０１は、公開鍵暗号装置４０２から供給される暗号鍵で、伝送システム４０３から入力されるデータに対して秘密鍵暗号の復号化を行い、復号化されたデータを出力端子２０４から出力する。乱数発生器４０１はランダムに数値を発生し、発生した数値を公開鍵暗号装置４０２に供給する。メモリ４０６には、予め入力端子４０７から公開鍵暗号の秘密鍵とそれに対応する公開鍵が入力されて記録されており、秘密鍵が公開鍵暗号装置４０２に供給され、公開鍵が出力端子４０５から出力される。通信装置の使用者が、設定した公開鍵を忘れてしまった場合には、通信装置の使用者は、設定した公開鍵を出力端子４０５から読み取る。公開鍵暗号装置４０２の入力端子４０８には、公開鍵暗号装置４０２の搭載された通信装置が呼び出しを行った側なのかあるいは呼び出しを受けた側なのかを示す制御信号が供給されている。公開鍵暗号装置４０２の入力端子４０４には公開鍵が供給される。入力端子４０４に供給される公開鍵は、通信相手の通信装置のメモリ４０６に記録されている公開鍵と等しいもので、通信装置の使用者が予め教えあっておくものとする。そして、公開鍵暗号装置４０２は、公開鍵暗号装置４０２の搭載された通信装置が呼び出しを行った側であれば、乱数発生器４０１の出力した数値を秘密鍵暗号装置２０１に供給するとともに、メモリ４０６から供給される秘密鍵で、乱数発生器４０１の出力した数値に対して公開鍵暗号の復号化を行い、入力端子４０４から供給される公開鍵で、前記復号化によって得られたデータに対して公開鍵暗号の暗号化を行い、暗号化によって得られたデータを伝送システム４０３に出力する。一方、公開鍵暗号装置４０２は、通信装置が呼び出しを受けた側であれば、メモリ４０６から供給される秘密鍵で、伝送システム４０３から入力されるデータに対して公開鍵暗号の復号化を行い、入力端子４０４から供給される公開鍵で、前記復号化によって得られたデータに対して公開鍵暗号の暗号化を行い、暗号化によって得られたデータを秘密鍵暗号装置２０１に供給する。伝送システム４０３は、秘密鍵暗号装置２０１から出力されるデータをもう一方の秘密鍵暗号装置２０１に供給するとともに、公開鍵暗号装置４０２から出力されるデータをもう一方の公開鍵暗号装置４０２に供給する。例えば公衆回線用のファクシミリにおいて図４の秘密情報通信装置を用いる場合には、伝送システム４０３は変復調装置と公衆回線網によって構成される。

【０００７】なお、図４の秘密情報通信装置では、公開鍵暗号にもとづく秘密情報通信装置といっても秘密鍵暗号によってデータの暗号化を行っているが、一般に、公開鍵暗号は暗号化や復号化の速度が秘密鍵暗号に比べて遅いので、図４のようにデータは秘密鍵暗号で暗号化されて伝送され、秘密鍵暗号で使われる暗号鍵が公開鍵暗号で暗号化されて伝送される。

【０００８】図５は、図４の秘密情報通信装置において使われる公開鍵暗号装置４０２の基本構成を示すブロック図である。図において、復号化回路５０２は、入力端子５０８から供給される秘密鍵で、入力端子５０９から入力されるデータに対して公開鍵暗号の復号化を行い、復号化によって得られたデータを暗号化回路５０３に供給する。なお、入力端子５０９には図４の乱数発生器４０１が出力する数値が、入力端子５０８には図４のメモリ４０６の出力する秘密鍵が供給されている。暗号化回路５０３は入力端子４０４から供給される公開鍵で、復号化回路５０２の出力に対して公開鍵暗号の暗号化を行い、暗号化によって得られたデータを出力端子５０６から出力する。出力端子５０６は図４の伝送システム４０３にデータを供給している。復号化回路５０４は、入力端子５０８から供給される秘密鍵で、入力端子５０７から入力されるデータに対して公開鍵暗号の復号化を行い、復号化によって得られたデータを暗号化回路５０５に供給する。入力端子５０６は図４の伝送システム４０３からデータを供給されている。暗号化回路５０５は、入力端子４０４から供給される暗号鍵で、復号化回路５０４から供給されるデータに対して公開鍵暗号のの暗号化を行い、暗号化によって得られたデータをセレクタ５０１に供給する。セレクタ５０１は、入力端子４０８から供給される制御信号が「通信装置が呼び出し側であること」を示していれば、入力端子５０９から供給されるデータを選択して出力端子５０５から出力し、一方、入力端子４０８から供給される制御信号が「通信装置が呼び出しを受けた側であること」を示していれば、暗号化回路５０５の出力を選択して出力端子５１０から出力する。出力端子５１０の出力は図４の秘密鍵暗号装置２０１に供給されている。

【０００９】なお、図５の公開鍵暗号装置で使われる公開鍵暗号としては、例えば、前記デビアスとプライスの著書において解説されているＲＳＡ（Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　ａｎｄ　Ａｄｌｅｍａｎ）暗号や、例えば１９９１年１２月に指宿で開催された第１４回情報理論

とその応用シンポジウムの予稿集の第９頁から１２頁に記載された島田著「もう一つの実用的な公開鍵暗号」において述べられている拡大ラビン暗号がある。また、拡大ラビン暗号の暗号化および復号化を実行するための回路の構成方法は、特願平３－２６８５１８号明細書の暗号通信符号化装置および復号化装置に記載されている。

【００１０】

【発明が解決しようとする課題】しかしながら、秘密鍵暗号にもとづく暗号通信装置だと、暗号鍵が第三者に知られると通信の内容が第三者によって解読され得るので、暗号鍵を第三者に盗み見されたり盗聴されないように、信頼できる人に直接運ばせたり暗号鍵を記録したメモを封筒に厳重に封印して郵送することが必要だった。このために、暗号鍵を管理するための労力が大きいという問題があった。

【００１１】公開鍵暗号にもとづく暗号通信装置では、公開鍵が第三者に知られても通信内容が解読されることはない。しかしながら、秘密鍵暗号の暗号鍵の長さが６４ビットだったのに対して公開鍵暗号の公開鍵は短いものでも５１２ビットなので、口頭で教えたり名刺の余白に印刷することは困難であった。また、公開鍵の長さが長いために、公開鍵を通信装置に手動入力することが使用者にとって大きな負担になるという問題があった。通信装置にＩＣカードの読み取り装置を搭載して公開鍵をＩＣカードに記録して配布すれば公開鍵を入力する負担を減らせめものの、通信装置のコストが大きくなるという問題があった。

【００１２】本発明の課題は、秘密にする必要が無くしかも桁数の短い数値を通信装置に設定するだけで、通信内容が第三者に解読できないようにする秘密情報通信方法を提供することにある。

【００１３】本発明の別の課題は、秘密にする必要が無くしかも桁数の短い数値を通信装置に設定するだけで、通信内容が第三者に解読できないようにする秘密情報通信装置を提供することにある。

【００１４】

【課題を解決するための手段】本発明によれば、データを秘密鍵暗号で暗号化して伝送し、秘密鍵暗号の暗号鍵を公開鍵暗号で暗号化して伝送する秘密情報通信方法において、少なくとも、公開鍵暗号の公開鍵を受信する受信ステップと、受信した公開鍵のハッシュ値を計算する計算ステップと、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを比較する比較ステップと、この比較ステップにおいて両ハッシュ値が一致しない時、通信を終了する通信終了ステップとを含むことを特徴とする秘密情報通信方法が得られる。

【００１５】更に、本発明よれば、前記通信終了ステップは、両ハッシュ値が一致しない時、通信終了指示を表示する表示ステップと、通信終了指示に応答して、通信を終了するステップとを、有することを特徴とする前述の秘密情報通信方法が得られる。

【００１６】又、本発明によれば、前記表示ステップは、両ハッシュ値が一致しない時、前記通信終了指示を可聴表示又は可視表示することを特徴とする前述の秘密情報通信方法が得られる。

【００１７】このように、予め通信相手から送られているハッシュ値と伝送された公開鍵のハッシュ値とが一致しなければ警報を発生して、通信を終了するか否かの判断を通信装置の使用者に行わせても良い。

【００１８】更に、前記比較ステップは、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを表示装置に表示させえて比較することを特徴とする前述の秘密情報通信方法が得られる。このように、予め通信相手から送られているハッシュ値と、伝送された公開鍵のハッシュ値とを表示装置に表示し、予め通信相手から送られているハッシュ値と伝送された公開鍵のハッシュ値との比較および通信を終了するか否かの判断を通信装置の使用者に行わせても良い。

【００１９】又、本発明によれば、データを秘密鍵暗号で暗号化して伝送し、秘密鍵暗号の暗号鍵を公開鍵暗号で暗号化して伝送する秘密情報通信装置において、少なくとも、公開鍵暗号の公開鍵を受信する受信手段と、受信した公開鍵のハッシュ値を計算する計算手段と、予め通信相手から送られているハッシュ値と前記計算ステップで計算された公開鍵のハッシュ値とを比較する比較手段と、この比較手段において両ハッシュ値が一致しない時、通信を終了する通信終了手段とを含むことを特徴とする秘密情報通信装置が得られる。

【００２０】

【作用】本発明では、もし盗聴者が公開鍵のハッシュ値を入手すると、原理的には、盗聴者がハッシュ値の一致するような整数を見つけ出し、その整数を公開鍵にもつような公開鍵暗号を生成できる。本発明では、公開鍵のハッシュ値のみを比較することで、受信した公開鍵が正規の通信相手から送られたものであるかどうかを確認しているので、正規の通信相手の公開鍵と盗聴者がそのようにして生成した公開鍵とを区別できない。従って盗聴者は、原理的には、正規の通信相手に成り済ましてデータを詐取できる。

【００２１】この問題を解決する方法としては、ハッシュ値の生成方法を通信相手ごとに変更することが考えられる。実際、例えば前記デビアスとプライスの文献によれば、ディジタル署名などの用途では、ハッシュ値の生成方法すなわちハッシュ関数の鍵が公開鍵暗号で暗号化されて、ハッシュ値と通信文とがいっしょに送信される。しかしながら、この方法では、暗号鍵の配送という問題が、ハッシュ関数の鍵の配送という問題に置き換えられるだけで意味が無い。また、ハッシュ関数の鍵を秘

密にすることも考えられるが、電話やファクシミリのように多数のメーカーによって製造され多数の装置が不特定多数に市販されている場合には、ハッシュ関数の鍵の秘密を守ることは困難である。

【００２２】しかしながら、実は、ハッシュ値の生成方法を固定しておいても、正規の通信相手に成り済ましてデータを詐取することは困難である。というのも、ハッシュ値の生成方法を知っている盗聴者は、ハッシュ値が正規の通信相手と等しくなるような整数を簡単に求められるかもしれないが、公開鍵暗号においては、公開鍵から秘密鍵を求めるためには膨大な計算量を要するので、そのような整数を見つけたとしても、その整数を公開鍵とするような公開鍵暗号の秘密鍵を求めることは事実上不可能だからである。盗聴者が所望のハッシュ値を有する公開鍵と秘密鍵の組を得るには、公開鍵暗号の秘密鍵を発生して、対応する公開鍵のハッシュ値を計数するという操作を、公開鍵のハッシュ値が正規の通信相手のものと等しくなるまで繰り返すしかない。ハッシュ値の長さを６４ビット程度に選んでおけば、スーパーコンピューターを使って計算しても何万年もかかるので、所望のハッシュ値を持つ公開鍵と秘密鍵の組み得ることは事実上不可能である。

【００２３】

【実施例】図１は本発明にもとづく秘密情報通信方法を実行する秘密情報通信装置の基本構成を示す機能ブロック図である。図において、秘密鍵暗号装置２０１、公開鍵暗号装置４０２、乱数発生器４０１、メモリ４０６は、図４の従来の公開鍵暗号にもとづく秘密情報通信装置と同様な処理を実行する。ただし、メモリ４０６から出力される公開鍵は、図４の出力端子４０５に出力されるのではなく、伝送システム１０２に供給される。また、公開鍵暗号装置４０２は、図４の入力端子４０４から公開鍵を供給されるのではなく、伝送システム１０２から公開鍵を供給される。そして、伝送システム１０２は、図４の伝送システム４０３が行っていた処理に加えて、一方の通信装置のメモリ４０６が出力する公開鍵を、もう一方の通信装置の公開鍵暗号装置４０２に供給する。伝送システム１０２から供給される公開鍵とメモリ４０６から供給される公開鍵は、セレクタ１０１にも供給されており、入力端子１０３に供給される制御信号に応じて、どちらか一方をハッシュ計算回路１０４に供給する。ハッシュ計算回路１０４は、セレクタ１０１から供給された公開鍵のハッシュ値を生成し、ハッシュ値を出力端子１０５と比較器１０８に供給する。比較器１０８はハッシュ計算回路１０４から供給されるハッシュ値と入力端子１０６から供給されるハッシュ値とを比較し、もし、両者が一致していなかったら警報信号を出力端子１０７から出力する。なお、通信装置の使用者は、予め、入力端子１０３の制御信号を操作してセレクタ１０１の出力としてメモリ４０６の出力を選択させ、メモリ４０６に記録された公開鍵のハッシュ値を出力端子１０５から得ておき、通信相手にそのハッシュ値を教えておく。そして、通信を行う際には、セレクタ１０１の出力として伝送システム１０２の供給する公開鍵を選択させ、入力端子１０６に通信相手から教えられたハッシュ値を入力する。もし、伝送システム１０２を介して接続している通信相手のメモリ４０６に記録されている公開鍵のハッシュ値と、所望の通信相手のメモリ４０６に記録されている公開鍵のハッシュ値とが異なっていれば、比較器１０７は警報信号を発生する。出力端子１０７から出力される警報信号は、秘密情報通信装置の搭載されている通信装置によっても異なるが、多くの用途では、伝送システム１０２に供給され、警報信号が発生したならば伝送システム１０２は通信を終了する。

【００２４】ただし、電話のように使用者自身がデータすなわち音声を発する通信装置では、出力端子１０７から出力される警報信号をブザーや発光ダイオードなどの表示装置に接続して、使用者に警報信号の有無を知らせ、通信を終了するか否かの判断を使用者に行わせることも可能である。また、電話のような通信装置では、比較器１０８を使わずに、ハッシュ計算回路１０４の出力を表示装置に表示して、ハッシュ計算回路の出力と通信相手のハッシュ値が一致するか否かの比較を使用者に行わせることも可能である。また、通信相手のハッシュ値を入力端子１０６から比較器１０８に直接供給せずに、通信相手のハッシュ値をメモリに記録しておき、メモリから比較器１０８に供給しても構わない。例えば、ファクシミリや電話などの通信装置では、予め使用者が通信相手の電話番号に続けて＃コードで区切ってハッシュ値の十進数表示を通信装置に入力して、通信装置はその数値をメモリに登録しておき、自動ダイヤルが実行された場合には、通信装置は＃コードに続いた数値を比較器１０８に供給することが考えられる。このようにすれば、通信を行うごとにハッシュ値を指定する必要が無くなるし、ハッシュ値が拡張された電話番号と見なせるので、秘密情報通信装置の搭載されていない電話やファクシミリを使っていたのとほぼ同様にして、秘密情報通信装置の搭載された電話やファクシミリを使える。

【００２５】なお、図１のハッシュ計算回路１０４で使われるハッシュ値の生成方法としては、例えば前記１９９２年１１月に水上で開催された情報理論とその応用シンポジウムの予稿集で述べられている多重剰余暗号を使うものがある。多重剰余暗号を使えば、暗号鍵のブロック長を選択するだけで、例えば長さ５１２ビットの公開鍵から長さ６４ビットのハッシュ値を生成できる。また、多重剰余暗号の暗号化および復号化を実行するための回路の構成方法は、前記特願平４－１２８４０９号明細書の暗号通信装置に記載されている。ただし、ハッシュ計算回路１０４ではハッシュ値の生成方法すなわちハッシュ計算回路の鍵を固定しておくので、予め決められ

た暗号鍵を記録しておくためのメモリが必要である。

【００２６】

【発明の効果】本発明の秘密通信方法及び装置では、以上で述べたように、通信装置に桁数の短いハッシュ値を指定するだけで、第三者に通信内容が解読されることなく通信できる。ハッシュ値は秘密にしておく必要が無いので、名刺などに印刷して公開したり電話を介して口頭で教えることも可能である。しかも、本発明の秘密通信方法及び装置は、従来の公開鍵暗号にもとづく秘密通信装置に公開鍵の伝送手順とハッシュ値を計算するための手段を付加するだけで済むので、実現がきわめて容易である。

【図面の簡単な説明】

【図１】本発明の秘密情報通信方法を実行する秘密情報通信装置の基本構成を示す機能ブロック図。

【図２】秘密鍵暗号にもとづく従来の秘密情報通信装置の基本構成を示す機能ブロック図。

【図３】図２の秘密情報通信装置の秘密鍵暗号装置２０１の基本構成を示す機能ブロック図。

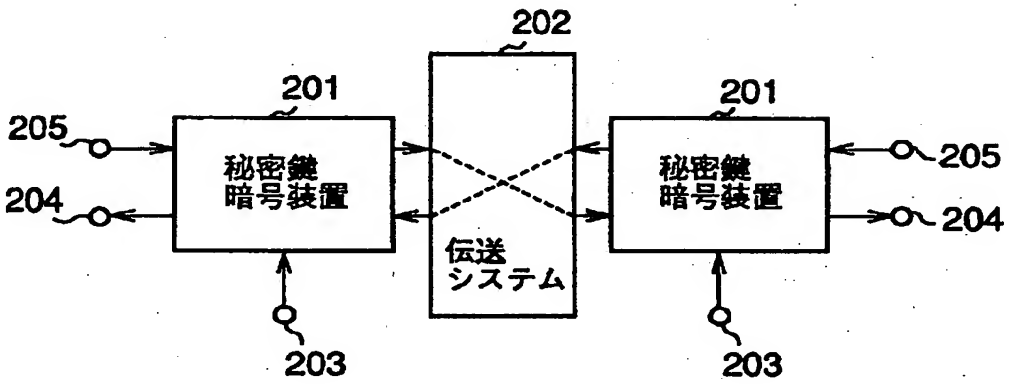
【図４】公開鍵暗号にもとづく従来の秘密情報通信装置の基本構成を示す機能ブロック図。

【図５】図４の秘密情報通信装置の公開鍵暗号装置４０２の基本構成を示す機能ブロック図。

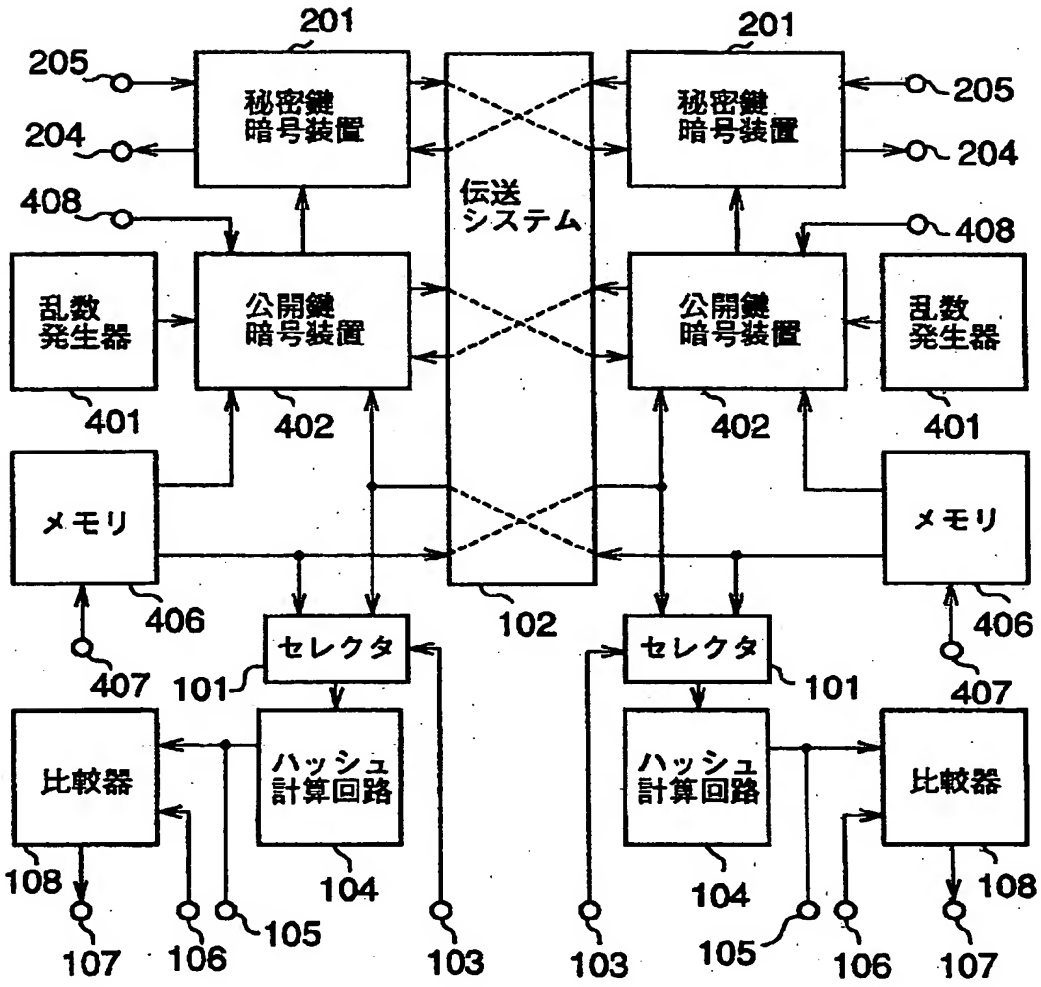
【符号の説明】

１０２	伝送システム
１０４	ハッシュ計算回路
１０８	比較器
２０１	秘密鍵暗号装置
２０２	伝送システム
４０１	乱数発生器
４０２	公開鍵暗号装置
４０３	伝送システム
４０６	メモリ

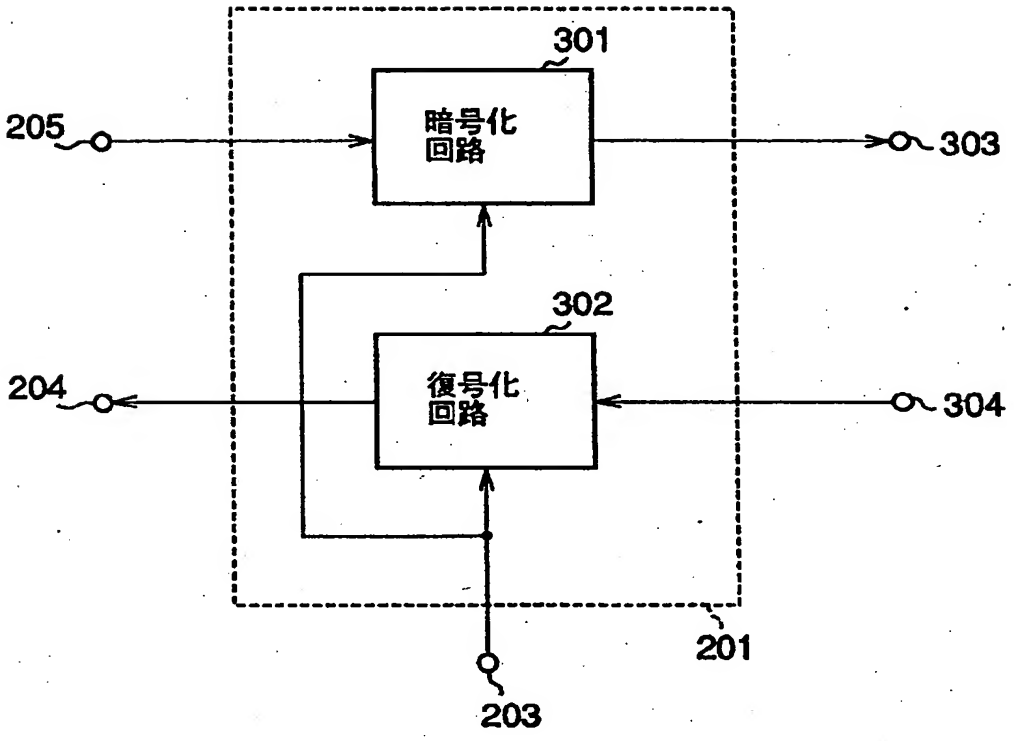
【図２】



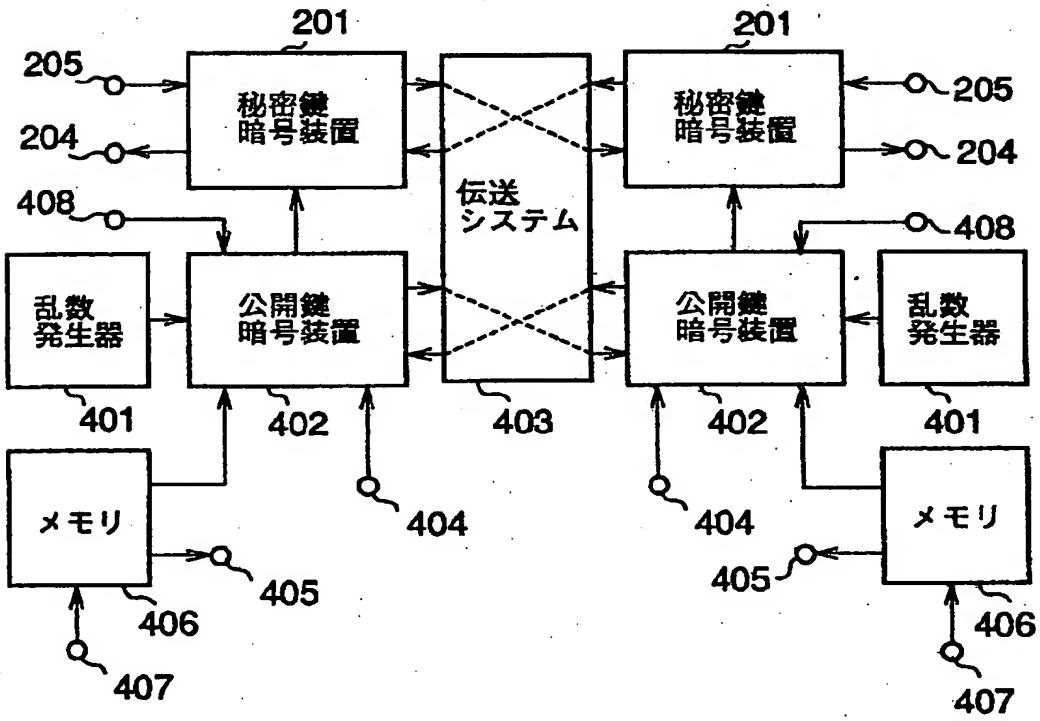
【図１】


201
201
205
204
秘密鍵
暗号装置
秘密鍵
暗号装置
205
204
408
伝送
システム
408
乱数
発生器
公開鍵
暗号装置
公開鍵
暗号装置
乱数
発生器
401
402
402
401
メモリ
メモリ
406
102
406
407
セレクタ
101
セレクタ
101
407
比較器
ハッシュ
計算回路
ハッシュ
計算回路
比較器
108
104
104
108
107
106
105
103
103
105
106
107

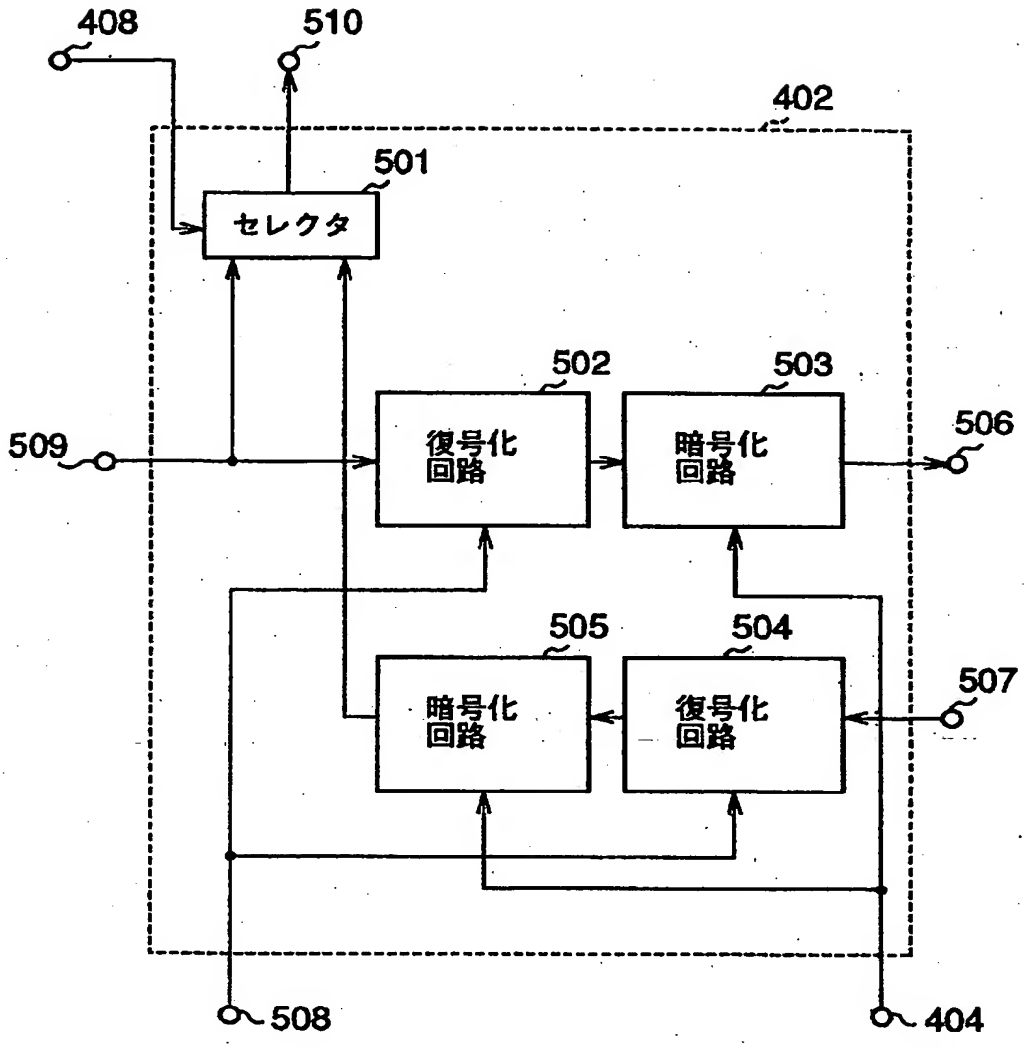
【図３】


301
暗号化
回路
205
303
302
復号化
回路
204
304
201
203

【図４】


201
201
205
秘密鍵
暗号装置
秘密鍵
暗号装置
205
204
204
伝送
システム
408
408
乱数
発生器
公開鍵
暗号装置
公開鍵
暗号装置
乱数
発生器
401
402
403
402
401
メモリ
404
404
メモリ
405
405
406
406
407
407

【図5】



フロントページの続き

(51) Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/10				
9/12				